

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-132457

(43)Date of publication of application : 10.05.2002

(51)Int.Cl.

G06F 3/06

G06F 12/14

G09C 1/00

G11B 20/10

H04N 5/91

(21)Application number : 2000-327591

(71)Applicant : VICTOR CO OF JAPAN LTD

(22)Date of filing : 26.10.2000

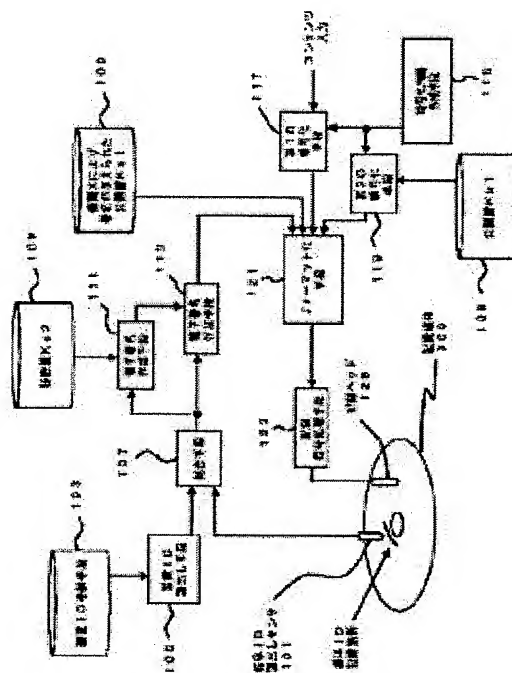
(72)Inventor : OISHI TAKESHI

## (54) INFORMATION RECORDING DEVICE, INFORMATION REPRODUCING DEVICE AND INFORMATION RECORDING/REPRODUCING DEVICE

### (57)Abstract:

**PROBLEM TO BE SOLVED:** To make it impossible to make a copy from a recording medium and to produce plural copied recording media even if a device ID of an information recording device with which contents have been recorded is stolen or illegally altered.

**SOLUTION:** To combined ID data, being stored in the device ID storing means 103 of the information recording device, which is a combination of the device ID that permits the information recording device to be identified or a group ID to which the information recording device belongs and a medium ID that permits the recording medium 300 to be identified, an electronic signature adding means 113 adds an electronic signature to generate data, which are stored in the recording medium together with the contents. Thereby, only if it is confirmed that the information reproducing device is the device identical with the information recording device with which the contents have been recorded or is the device belonging to the group which is set so that it can reproduce the contents, and that the contents are recorded on the recording medium identical with the recording medium on which the information recording device has recorded the contents, the contents can be reproduced.



Japanese Unexamined Patent Application Publication No. 2002-132457

# **SPECIFICATION <EXCERPT>**

[0039] Next, the determination of whether to permit a reproduction of content in Step S36 is described in detail. FIG. 7 is a flowchart showing an example of the operation for the determination of whether to permit a reproduction of content in Step S36 shown in the flowchart of FIG. 6. The operation regarding whether to permit a reproduction is performed in such a manner that a microcomputer in the information reproducing apparatus reads required data as appropriate into a memory in the microcomputer in the information reproducing apparatus. After Step S35, a flag P indicating whether to permit a reproduction is initialized and set to be  $P = 0$ . Here, the flag P indicating whether to permit a reproduction shows prohibiting a reproduction when  $P = 0$ , and shows permitting a reproduction when  $P = 1$ . Moreover, when the determination of whether to permit a reproduction is not completed, a reproduction is prohibited ( $P = 0$ ).

[0040] Next, in Step S42, whether or not an electronically signed public key Ks1 is authorized is determined using a public key Kx1 that the reproducing device has received from an organization X. Since the electronic signature that protects the public key Ks1 is created from a secret key Kx2 which cannot be known by people outside the organization X, it is impossible for a third party to create a correct electronic signature. Accordingly, even if the third party replaces a pair of the public key Ks1 and the secret key Ks2 with another pair without authorization, it is determined to be incorrect in this verification. When the public key Ks1 is determined to be incorrect in Step S42, the determination ends in Step S99 while the flag indicating whether to permit a reproduction remains  $P = 0$ , and decryption of the content is prohibited. In addition, in the case where the electronic signature is applied to concatenated data of the public key Ks1 and an

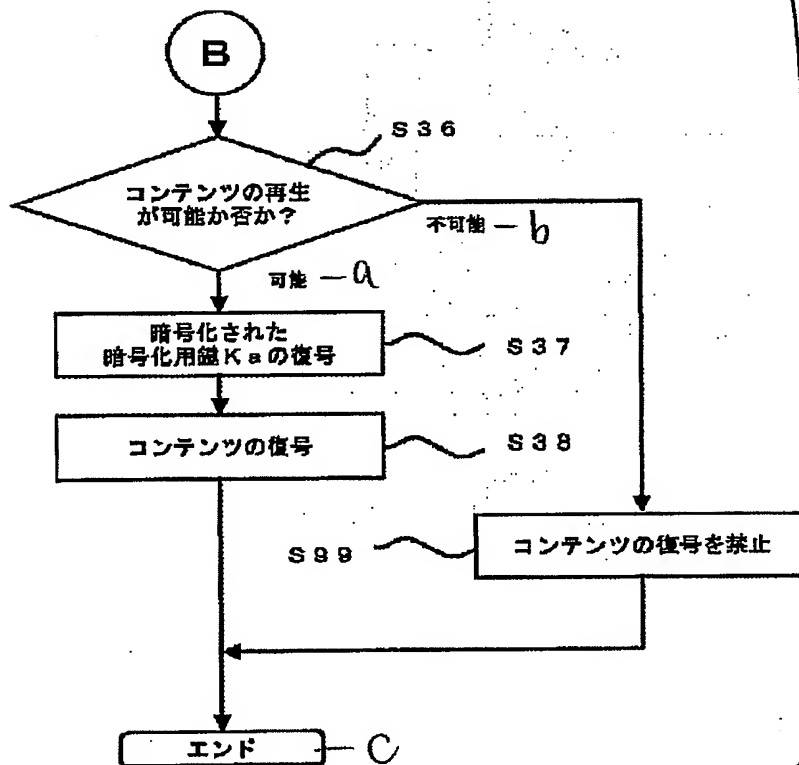
apparatus ID, it can be verified whether or not the public key Ks1 is reliably the public key for the apparatus in addition to whether or not the public key Ks1 itself is tampered, by verifying whether or not the concatenated data has correctly been transmitted.

[0041] When the public key Ks1 is determined to be correct in the verification in Step S42, in Step S43, it is determined whether or not the electronically signed concatenated ID data is authorized using the public key Ks1 determined to be authorized in Step S42. Even if the third party tampers the apparatus ID and a medium ID stored in a recording medium 300, it is determined to be incorrect in this verification. When the concatenated ID data is determined to be incorrect in Step S43, the determination ends in Step S99 while the flag indicating whether to permit a reproduction remains  $P = 0$ , and decryption of the content is prohibited.

[0042] When the concatenated ID data is determined to be correct in the verification in Step S43, in Step S44, the concatenated ID data is separated into the apparatus ID and the medium ID. Next, in Step S45, it is determined whether or not the apparatus ID of the information reproducing apparatus read out in Step S31 and the medium ID of the recording medium 300 read out in Step S32 are the same as the apparatus ID and the medium ID separated from the concatenated ID data in Step S44, respectively. When it is determined that the apparatus IDs and the medium IDs are both the same in Step S45, in Step S46, the flag P indicating whether to permit a reproduction is set to be  $P = 1$ . On the other hand, when both of the IDs or either pair is not the same, the determination ends in Step S99 while the flag indicating whether to permit a reproduction remains  $P = 0$ , and decryption of the content is prohibited. In addition, the flag P indicating whether to permit a reproduction is set as follows: when  $P = 1$ , a reproduction is permitted, and when  $P = 0$ , a reproduction is prohibited.

## DRAWINGS

FIG. 6



S36: Reproduction of content is permitted?

S37: Decrypt encrypted key Ka for encryption

S38: Decode content

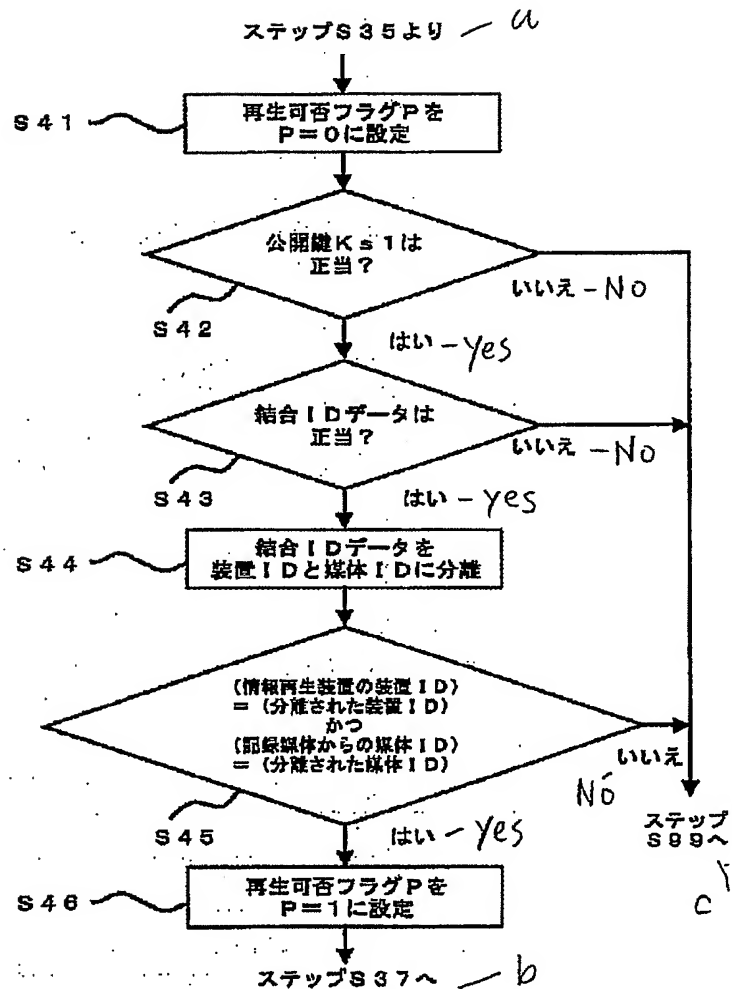
S99: Prohibit decoding of content

a: Permitted

b: Prohibited

c: End

FIG. 7



a: From Step S35

S41: Set flag P indicating whether to permit reproduction to be  $P = 0$

S42: Public key  $K_{s1}$  is authorized?

S43: Concatenated ID data is authorized?

S44: Separate concatenated ID data into apparatus ID and medium ID

S45: (apparatus ID of information reproducing apparatus = separated apparatus ID) and (medium ID of recording medium = separated medium ID)

S46: Set flag P indicating whether to permit reproduction to be  $P = 1$

b: To Step S37

c: To Step S99



## 【特許請求の範囲】

【請求項 1】 記録媒体の識別を可能とする媒体 I D を有する前記記録媒体にデジタルデータを記録するものであり、他の装置からの識別を可能とする装置 I D 又は他のグループに属する装置からの識別を可能とするグループ I D を有する情報記録装置であって、前記記録媒体から前記媒体 I D を読み出す手段と、前記情報記録装置から前記装置 I D 又は前記グループ I D を読み出す手段と、前記媒体 I D と前記装置 I D 又は前記グループ I D とを結合して、結合 I D データを作成する手段と、前記結合 I D データに電子署名を付加して、電子署名付き結合 I D データを作成する手段と、前記記録媒体に前記デジタルデータを記録する際、同時に前記電子署名付き結合 I D データを前記記録媒体に記録する手段とを、有する情報記録装置。

【請求項 2】 前記デジタルデータに関連して前記デジタルデータの保護の度合いを示す再生制約情報が存在し、前記再生制約情報に基づいて前記デジタルデータの再生条件を指定する指定情報を作成する手段と、前記デジタルデータの記録時に、同時に前記記録媒体に前記指定情報を記録する手段とを、有することを特徴とする請求項 1 記載の情報記録装置。

【請求項 3】 前記デジタルデータに関しては暗号化を行い、前記デジタルデータに付随する管理情報に関しては、すべての情報再生装置において読出し可能となるよう前記暗号化を行わないように制御することを特徴とする請求項 1 又は 2 記載の情報記録装置。

【請求項 4】 前記記録媒体に前記デジタルデータを記録する前に、前記デジタルデータを暗号化し、前記デジタルデータの前記暗号化に用いられた暗号化用鍵を暗号化して、前記記録媒体に記録することを特徴とする請求項 1 ないし 3 のいずれか 1 つに記載の情報記録装置。

【請求項 5】 デジタルデータと、前記デジタルデータを記録した情報記録装置の識別を可能とする装置 I D 又は前記情報記録装置が属するグループの識別を可能とするグループ I D と前記デジタルデータが記録された記録媒体の識別を可能とする媒体 I D とが結合されて電子署名が付加された電子署名付き結合 I D データとが記録された前記記録媒体から、前記デジタルデータを再生するものであり、他の装置からの識別を可能とする装置 I D 又は他のグループに属する装置からの識別を可能とするグループ I D を有する情報再生装置であって、前記記録媒体から前記媒体 I D を読み出す読出し手段と、前記記録媒体から前記デジタルデータと前記電子署名付き結合 I D データを読み出す手段と、前記電子署名付き結合 I D データに付加された電子署名を検証する第 1 の検証手段と、

前記電子署名付き結合 I D データから前記媒体 I D と前記装置 I D 又は前記グループ I D とを抽出する抽出手段と、前記情報再生装置が有する前記装置 I D 又は前記グループ I D と前記抽出手段によって抽出された前記装置 I D 又は前記グループ I D とが一致するか否かを検証する第 2 の検証手段と、前記読出し手段によって読み出された前記媒体 I D と前記抽出手段によって抽出された前記媒体 I D とが一致するか否かを検証する第 3 の検証手段と、前記第 1 から第 3 の検証手段による検証のうちのいずれか 1 つの検証結果が正しくない場合には、前記デジタルデータの再生を不可とする手段とを、有する情報再生装置。

【請求項 6】 前記記録媒体に記録されているデータから、前記デジタルデータに関連して前記デジタルデータの保護の度合いを示す再生制約情報を読み出し、前記再生制約情報に応じて前記デジタルデータの再生条件を設定する手段を有することを特徴とする請求項 5 記載の情報再生装置。

【請求項 7】 前記記録媒体に記録されているデータから、前記デジタルデータに付随する管理情報のみを読み出して、前記管理情報のみの出力を可能とすることを特徴とする請求項 5 又は 6 記載の情報再生装置。

【請求項 8】 前記デジタルデータが暗号化されており、さらに前記暗号化に用いられた暗号化用鍵が暗号化されて前記記録媒体に記録されている場合、前記記録媒体から読み出されたデータから前記暗号化用鍵を抽出し、前記情報再生装置が有する秘密鍵を用いて前記暗号化用鍵を復号し、前記復号された前記暗号化用鍵を用いて前記デジタルデータを復号することを特徴とする請求項 5 ないし 7 のいずれか 1 つに記載の情報再生装置。

【請求項 9】 記録媒体の識別を可能とする媒体 I D を有する前記記録媒体にデジタルデータを記録し、前記記録媒体から前記デジタルデータを再生するものであり、他の装置からの識別を可能とする装置 I D を有する情報記録再生装置であって、前記記録媒体に前記デジタルデータを記録するために、前記記録媒体から前記媒体 I D を読み出す手段と、前記情報記録装置から前記装置 I D を読み出す手段と、前記媒体 I D と前記装置 I D とを結合して、結合 I D データを作成する手段と、前記結合 I D データに電子署名を付加して、電子署名付き結合 I D データを作成する手段と、前記記録媒体に前記デジタルデータを記録する際、同時に前記電子署名付き結合 I D データを前記記録媒体に記録する手段とを有し、前記記録媒体から前記デジタルデータを再生するために、

前記録媒体から前記媒体 I D を読み出す読出し手段と、  
 前記録媒体から前記デジタルデータと前記電子署名付き結合 I D データを読み出す手段と、  
 前記電子署名付き結合 I D データに付加された電子署名を検証する第 1 の検証手段と、  
 前記電子署名付き結合 I D データから前記媒体 I D と前記装置 I D とを抽出する抽出手段と、  
 前記情報再生装置が有する前記装置 I D と前記抽出手段によって抽出された前記装置 I D とが一致するか否かを検証する第 2 の検証手段と、  
 前記読出し手段によって読み出された前記媒体 I D と前記抽出手段によって抽出された前記媒体 I D とが一致するか否かを検証する第 3 の検証手段と、  
 前記第 1 から第 3 の検証手段による検証のうちのいずれか 1 つの検証結果が正しくない場合には、前記デジタルデータの再生を不可とする手段とを、  
 有する情報記録再生装置。

【請求項 10】 前記デジタルデータに関連して前記デジタルデータの保護の度合いを示す再生制約情報が存在し、  
 前記録媒体に前記デジタルデータを記録する際に、  
 前記再生制約情報に基づいて前記デジタルデータの再生条件を指定する指定情報を作成し、前記デジタルデータの記録時に、同時に前記録媒体に前記指定情報を記録し、  
 前記録媒体から前記デジタルデータを再生する際に、  
 前記録媒体に記録されているデータから、前記デジタルデータに関連して前記デジタルデータの保護の度合いを示す再生制約情報を読み出し、前記再生制約情報に応じて前記デジタルデータの再生条件を設定することを特徴とする請求項 9 記載の情報記録再生装置。

【請求項 11】 前記録媒体に前記デジタルデータを記録する際に、  
 前記デジタルデータに関しては暗号化を行い、前記デジタルデータに付随する管理情報に関しては、すべての情報再生装置において読出し可能となるよう前記暗号化を行わないように制御して、  
 前記録媒体から前記デジタルデータを再生する際に、  
 前記録媒体に記録されているデータから、前記デジタルデータに付随する管理情報のみを読み出して、前記管理情報のみの出力を可能とすることを特徴とする請求項 9 又は 10 記載の情報記録再生装置。

【請求項 12】 前記録媒体に前記デジタルデータを記録する際に、  
 前記録媒体に前記デジタルデータを記録する前に、前記デジタルデータを暗号化し、前記デジタルデータの暗号化に用いられた暗号化用鍵を暗号化して前記録媒体に記録して、  
 前記録媒体から前記デジタルデータを再生する際に、

前記録媒体から読み出されたデータから前記暗号化用鍵を抽出し、前記情報再生装置が有する秘密鍵を用いて前記暗号化用鍵を復号し、前記復号された前記暗号化用鍵を用いて前記デジタルデータを復号することを特徴とする請求項 9 ないし 11 のいずれか 1 つに記載の情報記録再生装置。

#### 【発明の詳細な説明】

#### 【0001】

【発明の属する技術分野】本発明は、放送又は通信ネットワークを介して映像及び／又は音声のコンテンツについて、不正な複製や改変が行われないようコンテンツを保護するための情報記録装置及び情報再生装置並びに情報記録再生装置に関し、特に、特定の装置でコンテンツの再生を可能とするものに関する。

#### 【0002】

【従来の技術】従来、特に画質や音質の劣化なくコンテンツ（デジタルデータ）の複製が可能な記録においては、コンテンツの著作権の保護が課題となっていた。そこで、コンテンツに複製を制御するための信号（付加情報）を付加し、記録装置では必ずこの付加情報を参照して記録を制御するように取り決めることにより不法コピーを防止する技術や、機器間の伝送において、コンテンツに対して暗号化を行うことにより、伝送の途中の信号を盗み見てコンテンツを不法に取得及び利用することを防止する技術が提案されてきた。これらの技術は、著作権が存在するコンテンツが他の記録媒体に記録されることを禁止することで、不法コピーが行われて記録された記録媒体が作成されることを防止するものである。

【0003】また、例えばコンテンツを供給する従来の代表的な方法は、コンパクトディスク（CD）、デジタルビデオディスク（DVD）などのディスク記録媒体やビデオソフトテープなどの磁気記録媒体にコンテンツを記録して、その記録媒体を販売する形態である。この場合、コンテンツが記録された記録媒体と同種の記録媒体の再生が可能な再生装置であれば、どの装置でもその記録媒体の再生が可能であり、購入者は自宅の再生装置で記録媒体を再生して、コンテンツを楽しむことができる。

【0004】また、従来、コンテンツとともに装置 I D を記録してどの情報記録装置でコンテンツの記録が行われたかという記録を記録媒体中に残す方法も存在する。これにより、コンテンツを記録した情報記録装置に対応付けられた情報再生装置のみで、コンテンツの再生が可能となるようにすることができる。

#### 【0005】

【発明が解決しようとする課題】しかし、著作権保護に関する上記の従来技術は、基本的に記録媒体を販売する従来型の形態に対応したものであり、コンテンツが記録された記録媒体は、その種類の記録媒体の再生が可能な情報再生装置であれば、どの情報再生装置でも再生可能



なものである。そのため、特定の記録媒体に記録されたコンテンツが特定の装置でのみ再生できるようにすることはできない。

【0006】また、コンテンツとともに装置IDを記録してどの情報記録装置でコンテンツの記録が行われたかという記録を記録媒体中に残す方法に関しては、コンテンツの記録が行われた情報記録装置や不正に装置IDが改変された情報記録装置を用いれば、1つの記録媒体から複製を行い、複数の複製された記録媒体（デッドコピー）を作成することが可能である。この場合、例えばコンテンツを記録媒体に記録した情報記録装置の装置IDが不正に読み出されたり改変されたりした場合には、不正に改造された情報再生装置を用いて、簡単にコンテンツの不正な複製が可能となってしまう。

【0007】本発明は、上記問題点を鑑み、情報再生装置がコンテンツを記録した情報記録装置と同一の装置又は再生可能なように設定されてグループに属している装置であり、さらにコンテンツが情報記録装置で記録された記録媒体と同一の記録媒体に記録されていると確認できた場合のみ、コンテンツの再生を可能とすることを目的とする。

【0008】

【課題を解決するための手段】上記目的を達成するため、本発明は、コンテンツの記録の際に、そのコンテンツを記録する情報記録装置を識別可能とする装置ID又はその装置が属するグループを識別するグループIDと、そのコンテンツが記録されている記録媒体を識別可能とする媒体IDとを、コンテンツとともに記録媒体に記録する。また、コンテンツの再生の際に、記録媒体に記録されている装置ID又はグループIDと媒体IDとを参照して、コンテンツの再生が可能か否かを判定する。

【0009】すなわち、本発明によれば、記録媒体の識別を可能とする媒体IDを有する前記記録媒体にデジタルデータを記録するものであり、他の装置からの識別を可能とする装置ID又は他のグループに属する装置からの識別を可能とするグループIDを有する情報記録装置であって、前記記録媒体から前記媒体IDを読み出す手段と、前記情報記録装置から前記装置ID又は前記グループIDを読み出す手段と、前記媒体IDと前記装置ID又は前記グループIDとを結合して、結合IDデータを作成する手段と、前記結合IDデータに電子署名を付加して、電子署名付き結合IDデータを作成する手段と、前記記録媒体に前記デジタルデータを記録する際、同時に前記電子署名付き結合IDデータを前記記録媒体に記録する手段とを、有する情報記録装置が提供される。

【0010】また、本発明によれば、デジタルデータと、前記デジタルデータを記録した情報記録装置の識別を可能とする装置ID又は前記情報記録装置が属するグ

ループの識別を可能とするグループIDと前記デジタルデータが記録された記録媒体の識別を可能とする媒体IDとが結合されて電子署名が付加された電子署名付き結合IDデータとが記録された前記記録媒体から、前記デジタルデータを再生するものであり、他の装置からの識別を可能とする装置ID又は他のグループに属する装置からの識別を可能とするグループIDを有する情報再生装置であって、前記記録媒体から前記媒体IDを読み出す読み出し手段と、前記記録媒体から前記デジタルデータと前記電子署名付き結合IDデータを読み出す手段と、前記電子署名付き結合IDデータに付加された電子署名を検証する第1の検証手段と、前記電子署名付き結合IDデータから前記媒体IDと前記装置ID又は前記グループIDとを抽出する抽出手段と、前記情報再生装置が有する前記装置ID又は前記グループIDと前記抽出手段によって抽出された前記装置ID又は前記グループIDとが一致するか否かを検証する第2の検証手段と、前記読み出し手段によって読み出された前記媒体IDと前記抽出手段によって抽出された前記媒体IDとが一致するか否かを検証する第3の検証手段と、前記第1から第3の検証手段による検証のうちのいずれか1つの検証結果が正しくない場合には、前記デジタルデータの再生を不可とする手段とを、有する情報再生装置が提供される。

【0011】また、本発明によれば、記録媒体の識別を可能とする媒体IDを有する前記記録媒体にデジタルデータを記録し、前記記録媒体から前記デジタルデータを再生するものであり、他の装置からの識別を可能とする装置IDを有する情報記録再生装置であって、前記記録媒体に前記デジタルデータを記録するために、前記記録媒体から前記媒体IDを読み出す手段と、前記情報記録装置から前記装置IDを読み出す手段と、前記媒体IDと前記装置IDとを結合して、結合IDデータを作成する手段と、前記結合IDデータに電子署名を付加して、電子署名付き結合IDデータを作成する手段と、前記記録媒体に前記デジタルデータを記録する際、同時に前記電子署名付き結合IDデータを前記記録媒体に記録する手段とを有し、前記記録媒体から前記デジタルデータを再生するために、前記記録媒体から前記媒体IDを読み出す読み出し手段と、前記記録媒体から前記デジタルデータと前記電子署名付き結合IDデータを読み出す手段と、前記電子署名付き結合IDデータに付加された電子署名を検証する第1の検証手段と、前記電子署名付き結合IDデータから前記媒体IDと前記装置IDとを抽出する抽出手段と、前記情報再生装置が有する前記装置IDと前記抽出手段によって抽出された前記装置IDとが一致するか否かを検証する第2の検証手段と、前記読み出し手段によって読み出された前記媒体IDと前記抽出手段によって抽出された前記媒体IDとが一致するか否かを検証する第3の検証手段と、前記第1から第3の検証手段による検証のうちのいずれか1つの検証結果が正し

くない場合には、前記デジタルデータの再生を不可とする手段とを、有する情報記録再生装置が提供される。

【0012】

【発明の実施の形態】以下、図面を参照しながら、本発明の情報記録装置及び情報再生装置並びに情報記録再生装置について説明する。まず、情報再生装置がそのコンテンツを記録した情報記録装置と同一のものであり（すなわち、情報再生装置と情報記録装置が同一かつ一体化している情報記録再生装置）、さらに情報記録装置で記録された記録媒体と同一の記録媒体（すなわち、別の場所所でデータが複製されて記録された記録媒体を排除する）の場合のみ再生可能とする場合を説明する。

【0013】図1は、本発明の情報記録装置に係る一実施形態を示す模式図である。情報記録装置（情報記録再生装置の記録系）は、媒体ID読出しセンサ101、装置ID格納手段103、装置ID読出し手段105、結合手段107、鍵格納手段109、電子署名作成手段111、電子署名付加手段113、暗号化用鍵作成手段115、第1の暗号化手段117、第2の暗号化手段119、フォーマット化手段121、記録信号処理手段123、記録ヘッド125により構成されている。また、記録媒体300は、媒体ID読出しセンサ101及び記録ヘッド125が情報の読出し及び記録可能な位置に設置される。

【0014】媒体ID読出しセンサ101は、記録媒体300上にあらかじめ記録された媒体IDを読み出すための手段である。この媒体IDは、個々の記録媒体300に与えられた記録媒体300を識別するための識別情報であり、いったん記録媒体300に記録されると追記や消去、変更が不可能な識別情報である。媒体IDを記録媒体300に記録する方法としては、例えば特開2000-100068号公報に記載されているように、ディスクの「バースト・カッティング・エリア」に記録する方法がある。これは記録媒体300の製造時に、記録媒体300に強力なレーザーで媒体IDを記録するもので、一般ユーザによる改変はほぼ不可能である。

【0015】また、記録媒体300が半導体メモリである場合には、例えば情報を読み出そうとするとその情報が消えてしまうようなヒューザブルなエリアが情報記録領域とは別途用意され、この領域に媒体IDを記録することにより改変不可能にしたり、磁気ディスクに対して媒体ID記録用に書換え不可能なメモリを追加したりするなどの方法が考えられる。ここで、媒体IDの格納個所が書換え不可能なメモリの場合には、媒体ID読出し手段には図1のようなセンサを用いず、そのメモリのIDが格納されているアドレスを読み出すことにより、媒体IDの読出しが行われる。

【0016】装置ID格納手段103は、この情報記録装置内部にあらかじめ装置IDを格納しておくための手段である。この装置IDは、個々の情報記録装置に与え

られた情報記録装置を識別するための識別情報であり、この情報記録装置内部のメモリやハードウェアそのものに記録されるなど、情報記録装置の外部からは読出し不可能であり、いったん情報記録装置に記録されると追記や消去、変更が不可能な識別情報である。装置ID読出し手段105は、この装置IDを読み出すことが可能な手段である。

【0017】結合手段107は、媒体ID読出しセンサ101によって読み出された媒体ID、装置ID読出し手段105によって読み出された装置IDの2つのデータを結合して、1つの結合IDデータを作成する手段である。2つのデータの結合方法は、単に2つのデータを並べて1つの結合IDデータを作成する方法、2つのデータを所定の順序に並べて1つの結合IDデータを作成する方法、2つのデータに所定の演算を施して1つの結合IDデータを作成する方法など、どのような結合方法でも可能である。

【0018】鍵格納手段109は、秘密鍵Ks2、公開鍵Kb1、鍵の管理を行う機関Xにより署名が与えられた公開鍵Ks1（電子署名付き公開鍵Ks1）を格納するための手段である。図1では便宜上、それぞれの秘密鍵又は公開鍵に対して鍵格納手段が図示されているが、それぞれの鍵を格納する格納手段を設置することも可能であり、秘密鍵及び公開鍵をまとめて1つの格納手段に格納することも可能である。また、特に秘密鍵は情報記録装置外部から読出し不可能なように管理されて格納される必要があり、例えば、秘密鍵と公開鍵の格納手段をそれぞれ別々に設けて格納することも可能である。

【0019】秘密鍵Ks2とペアになる公開鍵Ks1には、各装置を管理している所定の機関Xにより、同機関Xが持っていて決して外部へは出さない秘密鍵Ks2を用いて作成された電子署名があらかじめ付加されている。また、この電子署名を公開鍵Ks1とこの装置IDを結合したデータとに対して作成するようにすることにより、公開鍵Ks1が他の装置で盗用された場合でも装置IDが異なっているので、盗用の発見が容易になる。

【0020】なお、一般にある秘密鍵で作成された電子署名が付加された情報は、その受信側または再生側で、受信または再生された電子署名が付加された情報に対して、その秘密鍵とペアとなる公開鍵を作用させて、所定の演算を施すことにより、受信または再生に至る途中のどこかで情報内容が改ざんされていないかを検証することが可能となる。その方法として、例えば文献N. Kovlitz, "Elliptic curve cryptosystems," Mathematics of Computation 48 (1987)203-209に記載されているECS P-D S A (Elliptic Curve Signature Primitive, DSA version.)といった技術を用いればよい。

【0021】電子署名作成手段111は、秘密鍵Ks2を用いて電子署名を作成する手段である。電子署名付加手段113は、結合手段107によって作成された結合

ＩＤデータに、電子署名作成手段１１１によって作成された電子署名を付加する手段である。暗号化用鍵作成手段１１５は、入力されたコンテンツを暗号化するための暗号化用鍵Ｋａを作成する手段であり、例えば暗号化用鍵となる乱数を発生させる乱数発生手段を用いることができる。この暗号化用鍵Ｋａは、各コンテンツに応じて、毎回異なる暗号化用鍵を作成する。第１の暗号化手段１１７は、暗号化用鍵作成手段１１５によって作成された暗号用鍵を用いて、入力されたコンテンツデータを暗号化する手段である。第２の暗号化手段１１９は、公開鍵Ｋｂ１を用いて暗号化用鍵作成手段１１５によって作成された暗号化用鍵を暗号化する手段である。なお、コンテンツは例えばデジタル放送などの放送ネットワークやインターネットなどの通信ネットワークを介して情報記録装置外部から配信されるものである。

【００２２】フォーマット化手段１２１は、電子署名が付加された結合ＩＤデータ、第１の暗号化手段によって暗号化されたコンテンツ、第２の暗号化手段によって暗号化された鍵Ｋａ、機関Ｘにより署名が与えられた公開鍵Ｋｓ１（電子署名付き公開鍵Ｋｓ１）を結合し、フォーマット化して１つのデータとする手段である。記録信号処理手段１２３は、フォーマット化手段１２１によって作成された１つのデータを記録媒体３００に記録可能となる信号に、例えば記録変調処理などの変換処理を行う手段である。記録ヘッド１２５は、記録信号処理手段１２３によって処理された信号を記録媒体３００に記録するための手段である。

【００２３】次に、図１に示す本発明の情報記録装置に係る記録媒体にコンテンツを記録する動作について説明する。図３及び図４は、本発明の情報記録装置に係る処理動作の一例を示すフローチャートの１枚目及び２枚目である。なお、図３及び図４は図中の「Ａ」と示された箇所であつてつながっている。

【００２４】まず、ステップＳ１１において、装置ＩＤ読出し手段１０５が、装置ＩＤ格納手段１０３からその情報記録装置を識別する装置ＩＤを読み出す。一方、ステップＳ１２において、媒体ＩＤ読出しセンサ１０１が、記録媒体３００からその記録媒体３００を識別する媒体ＩＤを読み出す。ステップＳ１３において、結合手段１０７が、これらの媒体ＩＤと装置ＩＤの２つのデータを結合して、１つの結合ＩＤデータを作成する。ステップＳ１４において、電子署名作成手段１１１が、ステップＳ１３で作成された結合ＩＤデータと鍵格納手段１０９に格納された秘密鍵Ｋｓ２とを用いて、結合ＩＤデータに対する電子署名を作成する。ステップＳ１５において、電子署名付加手段１１３が、ステップＳ１４で作成された電子署名を結合ＩＤデータに付加する。

【００２５】ステップＳ１６において、暗号化用鍵作成手段１１５がコンテンツを暗号化するための暗号化用鍵Ｋａを作成する。ステップＳ１７において、第１の暗号

化手段１１７が、ステップＳ１６で作成された暗号化用鍵Ｋａを用いて、情報記録装置に入力されたコンテンツを暗号化する。一方、ステップＳ１８において、ステップＳ１６で作成された暗号化用鍵Ｋａは第２の暗号化手段１１９にも入力されて、第２の暗号化手段１１９が、公開鍵Ｋｂ１を用いて暗号化用鍵Ｋａを暗号化する。

【００２６】そして、ステップＳ１３で作成された電子署名が付加された結合ＩＤデータ、ステップＳ１７で暗号化されたコンテンツ、ステップＳ１８で暗号化された暗号化用鍵Ｋａ、機関Ｘにより署名が与えられた電子署名付き公開鍵Ｋｓ１がフォーマット化手段１２１に入力されて、ステップＳ１９において、フォーマット化手段１２１が、これらのデータ（電子署名付き結合ＩＤデータ、暗号化されたコンテンツ、暗号化された暗号化用鍵Ｋａ、電子署名付き公開鍵Ｋｓ１）をフォーマット化して１つのデータとする。このとき、フォーマット化手段１２１は、これらのデータをそれぞれ所定のフォーマットの中の所定の場所に挿入する。

【００２７】なお、この電子署名付き結合ＩＤデータ、暗号化された暗号化用鍵Ｋａ、電子署名付き公開鍵Ｋｓ１をコンテンツの記録に付随したサブコードエリアやＡＵＸエリアに挿入したり、コンテンツに関連付けられた別のファイルとしたり、記録媒体３００に記録されたコンテンツを一括管理する一覧表のデータとして記録したりすることも可能である。また、このフォーマット化の際に、フォーマット化手段によって作成されたフォーマット化データには誤り訂正符号が付加されることが好ましい。

【００２８】ステップＳ２０において、記録信号処理手段１２３が、フォーマット化データに対して記録変調処理などの記録信号処理を行う。ステップＳ２１において、記録ヘッド１２５を用いて、ステップＳ２０で処理された信号を記録媒体３００に記録する。なお、記録媒体３００が半導体の場合には記録変調処理は省略されるなど、記録媒体３００の性質に適した方法で信号が記録される。

【００２９】次に、コンテンツ情報の記録媒体３００からの再生時の動作を説明する。図２は、本発明の情報再生装置に係る一実施形態を示す模式図である。情報再生装置（情報記録再生装置の再生系）は、媒体ＩＤ読出しセンサ２０１、装置ＩＤ格納手段２０３、装置ＩＤ読出し手段２０５、再生ヘッド２０７、再生信号処理手段２０９、データ抽出手段２１１、鍵格納手段２１３、再生可否判定手段２１５、第１の復号手段２１７、第２の復号手段２１９、制御手段２２１により構成されている。また、記録媒体３００は、媒体ＩＤ読出しセンサ２０１及び再生ヘッド２０７が情報の読出し可能な位置に設置される。

【００３０】媒体ＩＤ読出しセンサ２０１は、記録媒体３００上にあらかじめ記録された媒体ＩＤを読み出した

10

20

30

40

50

めの手段である。装置ID格納手段203は、この情報再生装置内部にあらかじめ装置IDを格納しておくための手段である。この装置IDは、個々の情報再生装置に与えられた情報再生装置を識別するための識別情報であり、この情報再生装置内部のメモリやハードウェアそのものに記録されるなど、情報再生装置の外部からは読出し不可能となるように記録されている。装置ID読出し手段205は、この装置IDを読み出すことが可能な手段である。

【0031】再生ヘッド207は、記録媒体300に記録された信号を読み出すための手段である。再生信号処理手段209は、再生ヘッドで読み出された信号を処理可能なデータに変換処理する手段である。データ抽出手段211は、再生信号処理手段209で処理されたデータに含まれている各データを選別及び抽出する手段である。鍵格納手段213は、公開鍵Kx1、秘密鍵Kb2を格納するための手段である。なお、図1と同様に、図2でも便宜上、それぞれの秘密鍵又は公開鍵に対して鍵格納手段213が図示されているが、秘密鍵及び公開鍵を1つの格納手段で行うことも可能であり、また、複数の格納手段を用いることも可能である。また、秘密鍵は情報再生装置外部から読出し不可能なように管理されて格納される必要がある。

【0032】再生可否判定手段215は、装置ID、媒体ID、電子署名付きKs1、電子署名結合IDデータなどを参照して、コンテンツの再生を可能とするか否かを判定し、その結果、例えばメモリなどの所定のアドレスに存在する再生可否フラグPをP=1（再生可能）とする処理を行う手段である。第1の復号手段217は、暗号化されたコンテンツを暗号化用鍵Kaを用いて、復号する手段である。なお、暗号化用鍵Kaは、コンテンツの暗号化の際に用いられた鍵であり、コンテンツを復号する場合、復号用鍵として用いられる。

【0033】第2の復号手段219は、暗号化された暗号化用鍵Kaを、秘密鍵Kb2を用いて復号する手段であり、これによって、第1の復号手段217で用いられる暗号化用鍵Kaが出力される。制御手段221は、再生可否判定手段215によって出力される結果（再生可否フラグPがP=0かP=1）に応じて、第1の復号手段217によるコンテンツの復号の動作を制御する手段である。なお、媒体ID読出しセンサ201、装置ID格納手段203、装置ID読出し手段205、鍵格納手段213は、それぞれ媒体ID読出しセンサ101、装置ID格納手段103、装置ID読出し手段105、鍵格納手段109と同じ機能を有する。

【0034】次に、図2に示す本発明の情報記録装置に係る記録媒体300に記録されたコンテンツを再生する動作について説明する。図5及び図6は、本発明の情報再生装置に係る処理動作の一例を示すフローチャートの1枚目及び2枚目である。なお、図5及び図6は図中の

「B」と示された箇所につながっている。まず、ステップS31において、装置ID読出し手段205が、装置ID格納手段203からその情報再生装置を識別する装置IDを読み出す。

【0035】一方、ステップS32において、媒体ID読出しセンサ201が、記録媒体300からその記録媒体300を識別する媒体IDを読み出し、ステップS33において、再生ヘッドが、記録媒体300に記録された信号を読み出す。なお、記録媒体300が半導体の場合には、媒体ID読出しセンサ201や再生ヘッド207を用いるのではなく、該当するアドレスの読出しを行うなどの記録媒体300に応じた処理が行われる。ステップS34において、再生信号処理手段209が、ステップS33で読み出された信号を処理可能なデータに変換処理する。ステップS35において、データ抽出手段211が、ステップS34で処理されたデータから、電子署名付き結合IDデータ、暗号化されたコンテンツ、暗号化された暗号化用鍵Ka、電子署名付き公開鍵Ks1を抽出する。

【0036】ステップS36において、再生可否判定手段215が、ステップS35で抽出された電子署名付き結合IDデータ、電子署名付き公開鍵Ks1、装置ID、媒体IDを参照して、コンテンツの再生（コンテンツの復号）が可能か否かを判定する。このステップS36における再生可否の判定や、再生の可否を示す再生可否フラグPに関しては、後で詳細に説明する。

【0037】ステップS36でコンテンツの復号が可能と判定された場合、再生可否フラグPが再生可能であることを示すP=1に設定される。ステップS37において、秘密鍵Kb2を用いて、第2の復号手段219がステップS35で抽出された暗号化された暗号化用鍵Kaを復号し、さらにステップS38において、復号された鍵Kaを用いて、第1の復号手段217が暗号化されたコンテンツを復号する。

【0038】一方、ステップS36でコンテンツの復号が不可能と判定された場合、ステップS99において、コンテンツの復号を禁止する。こうして得た判定結果により、P=1のときのみコンテンツ情報の再生を行い、例えば制御手段221が第1の復号手段によるコンテンツの復号の動作を制御して、コンテンツの復号が行われないようにする。また、制御手段221が、第2の復号手段219による暗号化鍵Kaの復号の動作を制御して、暗号化鍵Kaが復号されないようにし、その結果、コンテンツの復号が行われないようにすることも可能である。

【0039】次に、ステップS36におけるコンテンツの再生可否の判定に関して、詳細に説明する。図7は、図6に示すフローチャートのステップS36におけるコンテンツの再生可否の判定の動作の一例を示すフローチャートである。この再生可否に係る動作は、情報再生装

10

20

30

40

50

置のマイコンが適宜必要なデータを情報再生装置のマイコン内のメモリに取り込んで行うものである。ステップS35の後、まず、ステップS41において、再生可否フラグPを初期化して、P=0と設定する。ここで再生可否判定フラグPは、P=0のとき再生不可、P=1のとき再生可を表すフラグであり、再生可否判定が終了していない段階では再生は不可(P=0)とする。

【0040】次に、ステップS42において、電子署名付き公開鍵Ks1に対して、再生機器が機関Xから付与されて持っている公開鍵Kx1を用いて、公開鍵Ks1が正当なものか否かを判定する。公開鍵Ks1を保護している電子署名は機関X以外の者は知ることのできない秘密鍵Kx2により作成されているため、正しい電子署名を第三者が作成することはできない。したがって、第三者が、公開鍵Ks1と秘密鍵Ks2のペアを別のものに不正に入れ替えたとしても、この検証で正しくないと判定される。ステップS42で公開鍵Ks1が正しくないと判定された場合、再生可否フラグはP=0のまま、ステップS99において判定を終了し、コンテンツの復号を禁止する。なお、電子署名が公開鍵Ks1と装置IDとの結合データに対して施されている場合には、この結合データが正しく送られたことを検証することで、公開鍵Ks1そのものの改ざんの有無に加えて、確かにその装置のものであることが検証できる。

【0041】ステップS42の検証で公開鍵Ks1が正しいと判定された場合、ステップ43において、電子署名付き結合IDデータに対して、ステップS42で正当なものであると判定された公開鍵Ks1を用いて、結合IDデータが正当なものか否かを判定する。第三者が記録媒体300内に記録された装置IDと媒体IDを不正に書き換えたとしても、この検証で正しくないと判定される。ステップS43で結合IDデータが正しくないと判定された場合、再生可否フラグはP=0のまま、ステップS99において判定を終了し、コンテンツの復号を禁止する。

【0042】ステップS43の検証で結合IDデータが正しいと判定された場合、ステップS44において、結合IDデータを装置IDと媒体IDに分離する。次に、ステップS45において、ステップS31で読み出された情報再生装置の装置ID及びステップS32で読み出された記録媒体300の媒体IDと、ステップS44でID結合データから分離された装置ID及び媒体IDとがそれぞれ等しいか否かを判定する。ステップS45で装置ID及び媒体IDの両方ともが等しい場合、ステップS46において、再生可否フラグPをP=1とする。一方、両方又はどちらかが一方が等しくない場合、再生可否フラグはP=0のまま、ステップS99において判定を終了し、コンテンツの復号を禁止する。なお、この再生可否フラグPがP=1の場合には、コンテンツの再生が

不可能となるよう設定されている。

【0043】以上の動作は、コンテンツ(番組)ごとに行われ、コンテンツに装置ID及び媒体IDに関連させてコンテンツを記録するか否かを定めることが可能である。その結果、後述の再生動作により、あるコンテンツに関しては、同一の装置IDを有さない情報再生装置では読出し不可能とし、別のコンテンツに関しては、すべての情報再生装置で読出し可能とすることができる。すなわち、1つの記録媒体300に上記の動作による保護を受けたコンテンツと、保護のない一般的な記録条件で記録されたコンテンツとを共存させることが可能である。

【0044】また、上記の実施の形態では、情報再生装置がそのコンテンツを記録した情報記録装置と同一のものであり、さらに情報記録装置で記録された記録媒体300と同一の記録媒体300の場合のみ再生可能とする場合について説明したが、情報再生装置がそのコンテンツを記録した情報記録装置と同一のグループに属するものであり、さらに情報記録装置で記録された記録媒体300と同一の記録媒体300の場合のみ再生可能とすることも可能である。

【0045】ここで、同一のグループとは、情報記録装置と情報再生装置が同一の装置ではない場合でも、例えば同一のユーザが所有する複数の装置で構成するグループを特定するものである。例えばこのグループに属する情報再生装置に限って再生を許可するようにコンテンツを記録媒体300に記録する場合、記録媒体300にコンテンツとともにグループIDを記録する。そして、このグループ内の装置でグループIDを共有してそれぞれの装置内に格納しておき、記録媒体300中のグループIDが情報再生装置に格納されたグループIDと一致した場合のみ情報再生装置でコンテンツの再生が可能となるようにすればよい。

【0046】また、例えば各装置に装置IDが割り当てられているが、このとき同時にどのグループに属するものかを示すグループIDも付加されることによって、各装置にグループIDを割り当てることが可能となる。例えば、セキュアなデジタル出力と有効なコピープロテクション手段を持つ装置であるかどうかを示す情報が各装置の装置IDとともに格納されており、特定の機関Xがその情報群に署名したものが各装置に格納されることによって、グループ化されることになる。

【0047】このとき、装置IDにグループIDが付加されているため、図1及び図2の装置ID格納手段は装置ID+グループID格納手段と読み替えられ、図1及び図2の装置ID読出し手段は装置ID+グループID格納手段と読み替えられる。また、図3～7に示すフローチャートでは、装置IDは装置ID+グループIDと読み替えられ、ステップS45で装置IDが一致するか否かを検証する代わりに、グループIDが一致するか否



かを検証することによって、同一のグループに属する装置がコンテンツの再生を行えるようにすることが可能となる。

【0048】なお、再生されて出力されるコンテンツは、他の記録媒体300に記録される可能性がある。これを防ぐために、理想的にはデスクランブルされた後のデータはその後デコードされ、最終的にD/A変換されるまで一切LSIの外側に出なく、なおかつ、D/A変換出力には有効なコピープロテクション手段がなされている必要がある。この構成が実現できない場合でも、信号が流れる箇所にはユーザが簡単には触れられない構成（例えばBGAのLSIのピンから基板の内層を通して別のBGAのLSIのピンに接続されるなどの構成）とすることも可能である。また、コンテンツの出力に関しては、さらに暗号化して出力することも可能である。また、上記実施の形態では、第1の暗号化手段によってコンテンツの暗号化を行っているが、コンテンツの保護の度合いは大きく弱まるものの、このコンテンツの暗号化を行わないことも可能である。

【0049】さらに、コンテンツの供給者が、例えばコンテンツを記録媒体300に記録した情報記録装置と同一の情報再生装置（すなわち1つの情報再生記録装置）のみでしかコンテンツの読出しが不可能、コンテンツを記録媒体300に記録した情報記録装置と同一のグループに属する情報再生装置のみでしかコンテンツの読出しが不可能、どの情報再生装置でもコンテンツの読出しが可能などのコンテンツの保護条件を指定して、記録媒体300に記録したい場合がある。この場合、コンテンツの供給者は、コンテンツの供給とともに記録再生条件を指定する付加情報も同時に供給する必要がある。

【0050】また、管理情報とコンテンツとを分けて、管理情報に関しては暗号化が行われないようにしたい場合もある。この管理情報は、タイトル、記録時間などのコンテンツ中の番組の概要を示す情報を含んでいる。この管理情報が暗号化されずに直接読出し可能な形で記録媒体300に記録されている場合、この管理情報を再生することにより、記録媒体300にどのようなコンテンツが入っているか、どのくらいの容量を消費しているかななどの情報や、暗号化されている番組に関するタイトルや時間などの情報を簡単に利用することが可能となる。

【0051】次に、上記のコンテンツの供給者からの付加情報を受けて、コンテンツとともに管理情報を記録する動作について説明する。図8は、本発明の情報記録装置に係るコンテンツとともに管理情報を記録する一実施形態を示す模式図である。情報記録装置は、媒体ID読出しセンサ101、装置ID格納手段103、装置ID読出し手段105、結合手段107、鍵格納手段109、電子署名作成手段111、電子署名付加手段113、暗号化用鍵作成手段115、第1の暗号化手段117、第2の暗号化手段119、フォーマット化手段12

1、記録信号処理手段123、記録ヘッド125、データ分離手段127、管理情報作成手段129、メモリ131、入力選択手段133により構成されている。また、記録媒体300は、媒体ID読出しセンサ101及び記録ヘッド125が情報の読出し及び記録可能な位置に設置される。

【0052】次に、図8の各手段の動作について説明する。なお、図8に示す手段のうち図1に示す手段と同一の手段に関しては同一の参照番号が付されており、必要でない場合には説明を省略する。フォーマット化手段121は、第1の暗号化手段117によって暗号化されたコンテンツをフォーマット化して1つのデータとする手段である。データ分離手段127は、MPEGトランスポートストリームから付加情報とコンテンツとを分離する手段である。後述する再生制約フラグQの値に応じて管理情報を作成する手段である。メモリ131は、管理情報を一時的に保存する手段である。入力選択手段133は、暗号化されたコンテンツと管理情報の出力を切り替えて、記録信号処理手段123に出力する手段である。

【0053】次に、図8に示す本発明の情報記録装置に係るコンテンツとともに管理情報を記録する動作について説明する。図9は、本発明の情報記録装置に係るコンテンツとともに管理情報を記録する処理動作の一例を示すフローチャートである。例えば装置には、デジタル放送で使われているようなMPEGトランスポートストリームが入力されているものとする。

【0054】まず、ステップS51において、データ分離手段127が、MPEGトランスポートストリームから付加情報とコンテンツとを分離し、その付加情報を抽出する。付加情報には、タイトル、記録時間などのコンテンツ管理情報が含まれている。さらに、付加情報には、MPEGトランスポートストリームの作成の際に、コンテンツを再生する際の情報再生装置や記録媒体300に関して、制約を行うか否かの情報である再生制約情報が作成者によって挿入されている。

【0055】また、MPEGトランスポートストリームでは、情報はパケットで送られており、そのPID（パケットID）を参照することによって、そのパケットにどのようなデータが含まれているかがわかるようになっている。そして、コンテンツに含まれる番組に関して、どのPIDを有するデータが映像データ、音声データ、付加情報データのうちのどのデータを有しているかは、番組選択の情報であるPMT（Program Map Table：番組対応表）というパケットに記述されて送信される。したがって、このPMTを参照すれば、付加情報を抽出することが可能となる。

【0056】ステップS52において、ステップS51で分離された付加情報から再生制約情報を読み出し、ステップS53において、再生制約情報を参照して、同一

装置、同一の記録媒体 300 に制約するよう指定されているか否かを判断する。この再生制約情報は、コンテンツの供給者又は作成者が決定した著作権の保護条件を示す情報である。同一装置、同一の記録媒体 300 に制約するよう指定されていると判断された場合、ステップ S 54 において、再生制約フラグ Q が、同一装置、同一の記録媒体 300 に制約することを示す  $Q = 11$  に設定され、ステップ S 55 において、管理情報作成手段は  $Q = 11$  の値に応じて管理情報 TypeI を作成する。

【0057】一方、ステップ S 53 で同一装置、同一の記録媒体 300 に制約するよう指定されていないと判断された場合、ステップ S 56 において、再生制約情報を参照して、同一グループ、同一の記録媒体 300 に制約するよう指定されているか否かを判断する。同一グループ、同一の記録媒体 300 に制約するよう指定されていると判断された場合、ステップ S 57 において、再生制約フラグ Q が、同一グループ、同一の記録媒体 300 に制約することを示す  $Q = 10$  に設定され、ステップ S 58 において、管理情報作成手段は  $Q = 10$  の値に応じて管理情報 TypeII を作成する。

【0058】そして、ステップ S 59 において、ステップ S 55 で作成された管理情報 TypeI 又はステップ S 58 で作成された管理情報 TypeII をメモリに記憶する。さらに、ステップ S 60 において、第 1 の暗号化手段はコンテンツを暗号化し、暗号化されたコンテンツを記録媒体 300 に記録する。

【0059】一方、ステップ S 56 で同一グループ、同一の記録媒体 300 に制約するよう指定されていないと判断された場合、ステップ S 61 において、再生制約フラグ Q が装置の制約を行わないことを示す  $Q = 00$  に設定され、ステップ S 62 において、管理情報作成手段は、 $Q = 00$  の値に応じて管理情報 TypeIII を作成する。そして、ステップ S 63 において、ステップ S 62 で作成された管理情報 TypeIII をメモリに記憶する。ステップ S 64 において、第 1 の暗号化手段を制御して、コンテンツの暗号化が行われないようにして、コンテンツを記録媒体 300 に記録する。その後、ステップ S 65 において、ステップ S 62 で作成された管理情報 TypeIII を記録媒体 300 の管理情報エリアに記録する。

【0060】なお、再生制約フラグ Q の値に応じて、管理情報として入れなければならない情報が異なるので、再生制約フラグ Q の値が異なれば、例えば管理情報の内容が異なったり、管理情報内に存在する情報の意味が異なったりする。以下に、この管理情報について説明する。図 10 は、管理情報 TypeI、管理情報 TypeII、管理情報 TypeIII の一例を示す図である。なお、この実施の形態では、再生制約フラグ  $Q = 11$  の場合には管理情報 TypeI、再生制約フラグ  $Q = 10$  の場合には管理情報 TypeII、再生制約フラグ  $Q = 00$  の場合には管理情報 TypeIII が作成されるものとする。

【0061】管理情報について、具体例としては、例えば図 10 の (a) 管理情報 TypeI、(b) 管理情報 TypeII、(c) 管理情報 TypeIII が考えられる。記録する各番組について、これらの管理情報が作成され、記録媒体 300 内の管理情報エリアに記録される。管理情報には、番組番号、タイトル、信号仕様、記録仕様、記録位置情報、記録時間情報の 6 つの TypeI ~ III に共通した情報と、再生制約フラグ Q 及び再生制約フラグ Q の値に応じた様々な情報が含まれている。

【0062】番組番号は、記録媒体 300 に記録された番組を区別する整理番号である。タイトルは、入力される MPEG トランスポートストリーム中の付加情報として送られてくるタイトル情報である。このタイトルに関しては、ユーザが情報記録装置において入力することも可能である。信号仕様は、コンテンツの転送レートや圧縮のパラメータなどの信号仕様のデータである。記録仕様は、記録において高品質モードと標準モードといった記録レートの違いや、音声のチャンネル数などについていくつかの仕様が有る場合、それらのうちのどの条件で記録したのかを示す情報である。

【0063】また、記録位置情報は、例えば記録媒体 300 が細かいセクターに分かれている時に、セクターのうちのどこからどこまでがこのコンテンツの記録に割り当てられているかを示す情報である。なお、ディスクの場合には記録するセクターは離れた位置に存在することも可能であり、書き込み可能なセクターが制御手段などによって選択される。記録時間情報は、このコンテンツの全記録時間を示す情報である。これらの記録位置及び時間情報はコンテンツの記録中に逐次更新され、コンテンツの記録が終了した時点での情報が管理情報として記録媒体 300 に記録される。なお、途中でコンテンツの記録を中止したときは、それまでの記録時間が記録時間情報として記録される。以上が管理情報 TypeI ~ III に共通した情報である。

【0064】一方、再生制約フラグ Q は、上記のフローチャートによって定められた再生時の制約を示すフラグであり、再生時の制約条件に従って異なる値となっている。この再生制約フラグ Q は 3 つのタイプに分かれており、この値に応じて、この後に続くデータの有無やデータの意味などが異なってくる。

【0065】図 10 中の (a) に示す管理情報は、情報再生装置がそのコンテンツを記録した情報記録装置と同一のものであり、さらに情報記録装置で記録された記録媒体 300 と同一の記録媒体 300 の場合のみ再生可能とすることを示す再生制約フラグ  $Q = 11$  を有するものである。この管理情報には、電子署名付き結合 ID データ、公開鍵  $Ks1$  が含まれ、さらに、コンテンツが暗号化されるか否か（コンテンツの暗号化の有無）の情報が入り、コンテンツの暗号化が行われる場合には、管理情報には暗号化された暗号化用鍵  $Ka$  が含まれる。一方、

コンテンツが暗号化されない場合には、暗号化された暗号化用鍵K aが入るべき項目には、例えばオール0などの所定のダミーデータが入られるか、または、この項目が省略される規定とすることも可能である。

【0066】一方、図10中の(b)に示す管理情報は、情報再生装置がそのコンテンツを記録した情報記録装置と同一のグループに属するものであり、さらに情報記録装置で記録された記録媒体300と同一の記録媒体300の場合のみ再生可能とすることを示す再生制約フラグQ=10を有するものである。

【0067】この場合、管理情報には機器グループ情報が追加される。ここで、機器グループ情報は、例えば機関Xが各機器に対して与えられる情報である。また、コンテンツを供給する側は、コンテンツの配信において、付加情報中にコンテンツの再生を認めるグループを指定しておき、その情報を機器グループ情報として記述しておく。そして、コンテンツを例えばMPEGトランスポートストリームに変換するとき、この機器グループ情報を付加情報としてコンテンツとともに記録し、この機器グループ情報を参照して再生を許可する機器のグループを図10(b)の機器グループ情報の項目に記述する。一方、再生の際には、この機器グループ情報の記述内容により、今再生しようとしている情報再生装置が再生が許可されたグループに属する場合のみ再生を行うようにする。

【0068】一方、図10中の(c)に示す管理情報は、特に情報再生装置を制約せずに、すべての情報再生装置で再生可能とすることを示す再生制約フラグQ=00を有するものである。したがって、特に制約を設けないので、電子署名付き結合IDデータ、公開鍵K s 1情報などは必要なく、それらの項目も設けられていない。一方、コンテンツを暗号化するか否かの選択が可能となるように、コンテンツの暗号化の有無の項目と、暗号化された暗号化用鍵K aの項目が存在する。コンテンツを暗号化するか否かの選択は、コンテンツの供給者の付加情報による指定に従うようにすることが可能であるが、一般にはコンテンツの暗号化は行わないようにして、ユーザがそのコンテンツを他人に再生されたくない場合に、ユーザの指定により暗号化を行うような機能を情報記録装置に持たせることも可能である。

【0069】また、図9に示すのフローチャートでは、管理情報を最後に記録媒体300に記録しているが、コンテンツの記録に先立って記録可能な項目に関しては記録しておき、記録位置情報や記録時間情報などに関しては、コンテンツの記録に割り込む形で記録を更新していくようにすることも可能である。また、付加情報に記録される再生条件の指定は、個々の番組について行われるため、同一の記録媒体300上に記録されている番組について再生条件を変えて記録することも可能であり、1つの記録媒体300中に暗号化されている番組と暗号化

されていない番組とを混在させることも可能である。

【0070】次に、図9の情報記録装置で記録されたコンテンツ及び管理情報を再生する動作について説明する。図11は、本発明の情報再生装置に係るコンテンツ及び管理情報が記録された記録媒体を再生する一実施形態を示す模式図である。なお、図11を構成する手段は、図1を構成する手段と同一である。データ抽出手段によってコンテンツ及び管理情報が抽出され、コンテンツは図5及び図6のフローチャートに示す動作によって復号され、一方、管理情報は暗号化されていないので、そのまま出力することが可能である。

【0071】すなわち、同一の装置でのみ再生することを許可するか否かの指定を示す付加情報が記録されている場合、再生時にはまずこの付加情報を読み出す。そして、この付加情報の内容によって、同一又は同一のグループの装置でのみ再生が許可されている場合には図5及び図6のフローチャートにおける判定に従って、再生処理を行う。一方、他の装置による再生も許可されている場合には、図5及び図6のフローチャートにおける判定処理は行わないか、または、同一媒体に記録された他のコンテンツの再生のために判定処理は行っても、このコンテンツに関しては判定結果にかかわらず再生を行う。また、コンテンツが暗号化されているか否かによって、暗号化されたコンテンツの復号処理を行うか否かの処理を切り替えることも可能である。

【0072】また、タイトルや時間情報などは、コンテンツ一覧画面の画像情報に変換されてディスプレイに出力されることも可能であり、これによって、ユーザは記録媒体300にどのようなコンテンツが記録されているかを知ることが可能となる。このとき、上記の電子署名の照合で記録時と再生時で装置又は記録媒体300が異なっており、コンテンツの復号が不可能となっているコンテンツについては、そのコンテンツは内容を再生できないことを示すマークを付けるなどの方法で、ユーザに知らせることが可能である。

【0073】また、電子署名の照合で記録時と再生時で装置も記録媒体300も一致していることが確認されたときでも、コンテンツ一覧画面において、他の装置でも再生可能か否かを示すマークの表示を行うことも可能である。このように、ユーザに対して再生可否の分類を表示することにより、ユーザがそのコンテンツに関する制限を知ることが可能となり、例えば他の情報再生装置でも再生できると思って、実際に他の情報再生装置での再生を試みたが再生がうまく行えなかったというようなトラブルを防止できる。

【0074】また、管理情報を再生する際に、記録媒体300に複数のコンテンツが存在し、それらが複数の情報記録装置によって記録されたものである場合、情報記録装置毎に記録内容を分類して表示する機能を持たせることも可能である。



## 【0075】

【発明の効果】以上説明したように、コンテンツの記録の際に、そのコンテンツを記録する情報記録装置を識別可能とする装置ID又は情報記録装置が属するグループを識別可能とするグループIDと、そのコンテンツを記録する記録媒体を識別可能とする媒体IDとを、コンテンツとともに記録媒体に記録するので、どの情報記録装置又はどのグループに属する情報記録装置によってどの記録媒体にコンテンツが記録されたかという情報を、コンテンツとともに記録媒体に記録することが可能となる。

【0076】また、コンテンツの再生の際に、コンテンツとともに記録されている装置ID又はグループIDと媒体IDの2つのパラメータを参照して、コンテンツの再生可否の判定を行うので、2重にコンテンツを保護し、コンテンツが不正に複製されることを防ぐことが可能となる。

【0077】また、コンテンツの記録の際に、そのコンテンツを記録する情報記録再生装置を識別可能とする装置IDと、そのコンテンツを記録する記録媒体を識別可能とする媒体IDとを、コンテンツとともに記録媒体に記録し、コンテンツの再生の際に、記録媒体に記録されている装置IDがこの情報記録再生装置の装置IDと同一であり、かつ情報記録再生装置で記録された記録媒体と同一の記録媒体である場合のみコンテンツの再生を可能とするので、ただ1つの情報記録再生装置でのみ再生が可能となるように、記録媒体にコンテンツを記録することが可能となる。

【0078】また、情報記録装置にコンテンツを供給する際に、コンテンツとそれに関連する付加情報が供給されて、その付加情報を基にしてコンテンツの記録条件の制御を行うので、例えばコンテンツの供給者又は作成者により、コンテンツの記録再生条件を指定することが可能となり、コンテンツに存在する著作権の保護の度合いをコンテンツの供給者又は作成者が指定することが可能となる。

【0079】また、コンテンツの記録の際に、そのコンテンツのタイトルや時間情報などを示す管理情報に関しては、従来の再生方法で読出し可能なように記録するので、その記録媒体にどのようなコンテンツがどの時間位置に記録されているか、記録媒体の残り容量はどれくらいかなどのコンテンツの記録に付随して発生する管理情報を、すべての情報再生装置において確認することが可能となる。

## 【図面の詳細な説明】

【図1】本発明の情報記録装置に係る一実施形態を示す模式図である。

【図2】本発明の情報再生装置に係る一実施形態を示す

模式図である。

【図3】本発明の情報記録装置に係る処理動作の一例を示すフローチャートの1枚目である。

【図4】本発明の情報記録装置に係る処理動作の一例を示すフローチャートの2枚目である。

【図5】本発明の情報再生装置に係る処理動作の一例を示すフローチャートの1枚目である。

【図6】本発明の情報再生装置に係る処理動作の一例を示すフローチャートの2枚目である。

【図7】図6に示すフローチャートのステップS36におけるコンテンツの再生可否の判定の動作の一例を示すフローチャートである。

【図8】本発明の情報記録装置に係るコンテンツとともに管理情報を記録する一実施形態を示す模式図である。

【図9】本発明の情報記録装置に係るコンテンツとともに管理情報を記録する処理動作の一例を示すフローチャートである。

【図10】管理情報TypeI、管理情報TypeII、管理情報TypeIIIの一例を示す図である。

【図11】本発明の情報再生装置に係るコンテンツ及び管理情報が記録された記録媒体を再生する一実施形態を示す模式図である。

## 【符号の説明】

101、201 媒体ID読出しセンサ

103、203 装置ID格納手段

105、205 装置ID読出し手段

107 結合手段

109、213 鍵格納手段

111 電子署名作成手段

113 電子署名付加手段

115 暗号化用鍵作成手段

117 第1の暗号化手段

119 第2の暗号化手段

121 フォーマット化手段

123 記録信号処理手段

125 記録ヘッド

127 データ分離手段

129 管理情報作成手段

131 メモリ

133 入力選択手段

207 再生ヘッド

209 再生信号処理手段

211 データ抽出手段

215 再生可否判定手段

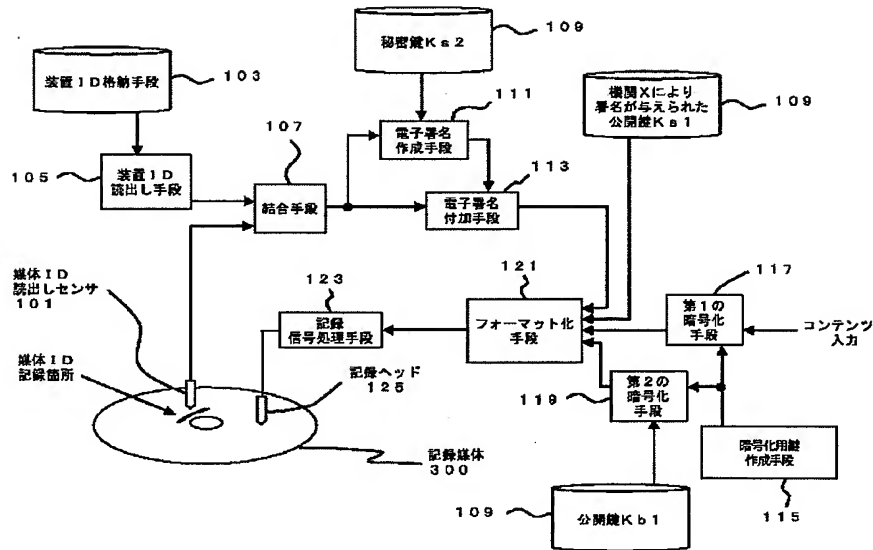
217 第1の復号手段

219 第2の復号手段

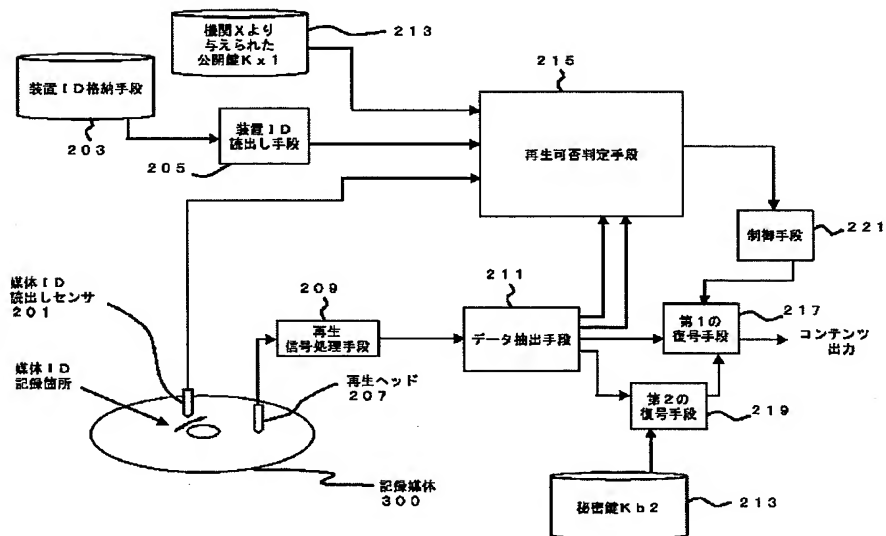
221 制御手段

300 記録媒体

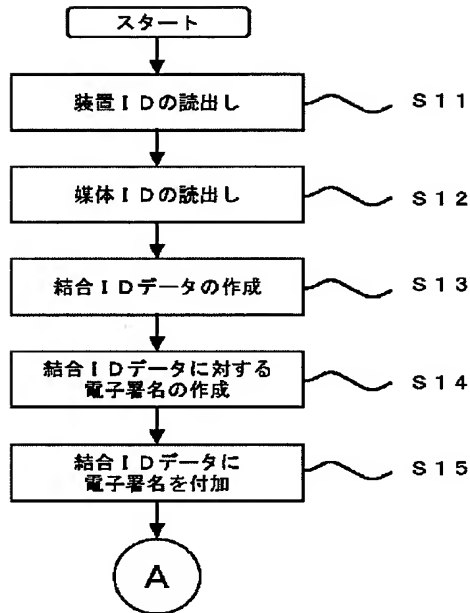
【図1】



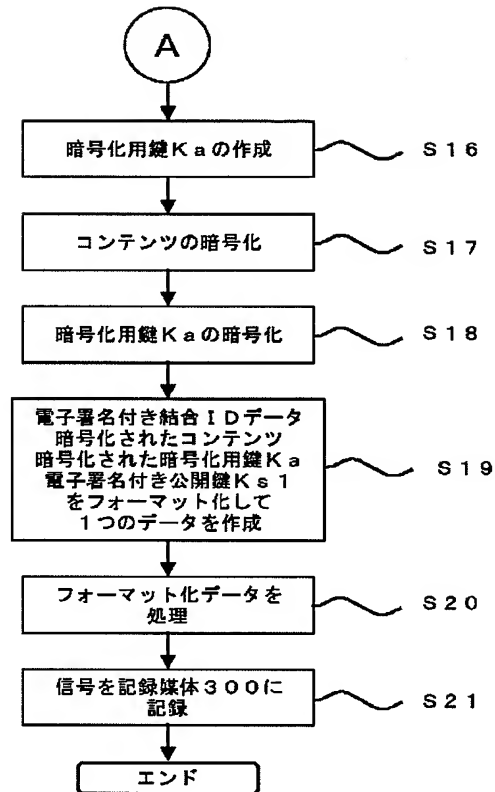
【図2】



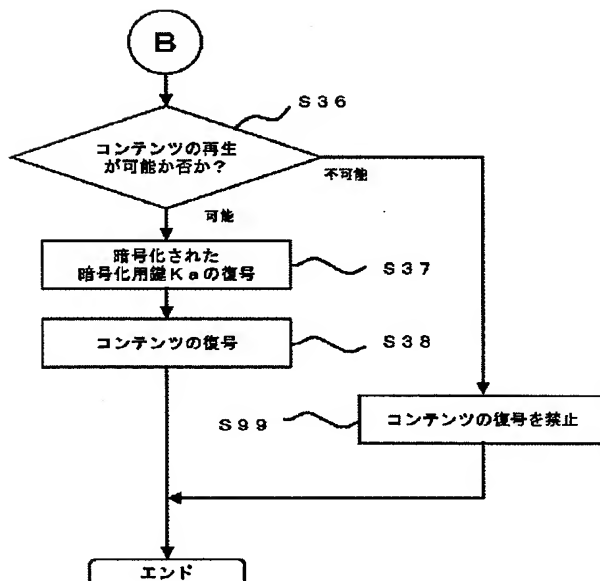
【図3】



【図4】



【図6】



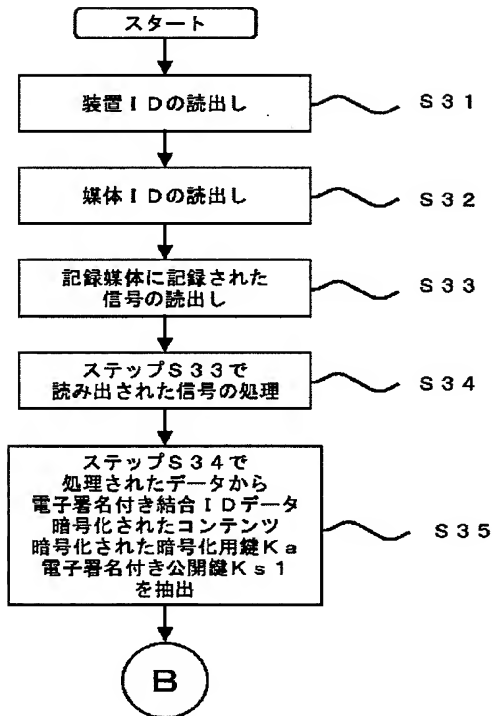
【図10】

(a) Type I	(b) Type II
番組番号	番組番号
タイトル	タイトル
信号仕様	信号仕様
記録仕様	記録仕様
再生制約情報 (Q=11)	再生制約情報 (Q=10)
電子署名付き結合ID情報	電子署名付き結合ID情報
公開鍵Ks1情報	機器グループ情報
コンテンツの暗号化の有無	公開鍵Ka1情報
暗号化された暗号化用鍵Ka	コンテンツの暗号化の有無
記録位置情報	暗号化された暗号化用鍵Ka
記録時間情報	記録位置情報
	記録時間情報

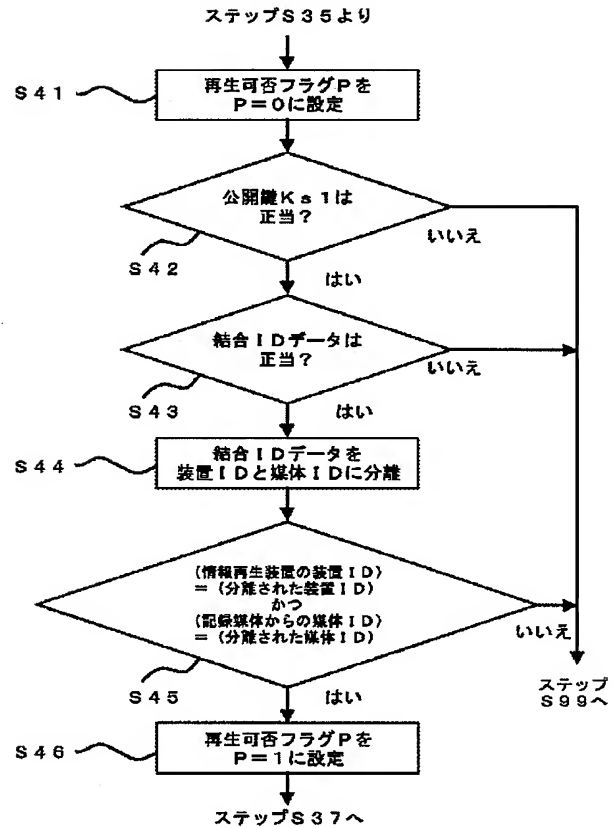
  

(c) Type III
番組番号
タイトル
信号仕様
記録仕様
再生制約情報 (Q=00)
コンテンツの暗号化の有無
暗号化された暗号化用鍵Ka
記録位置情報
記録時間情報

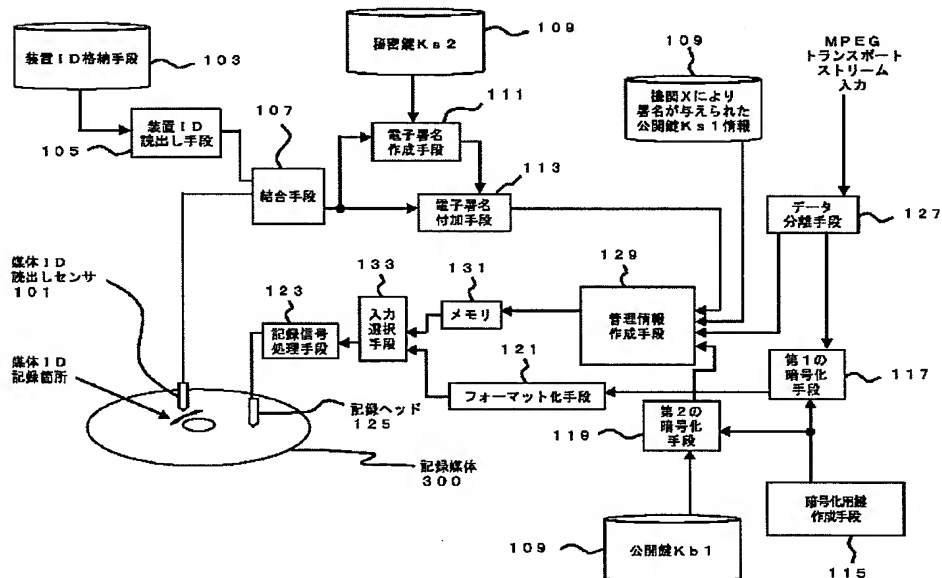
【図 5】



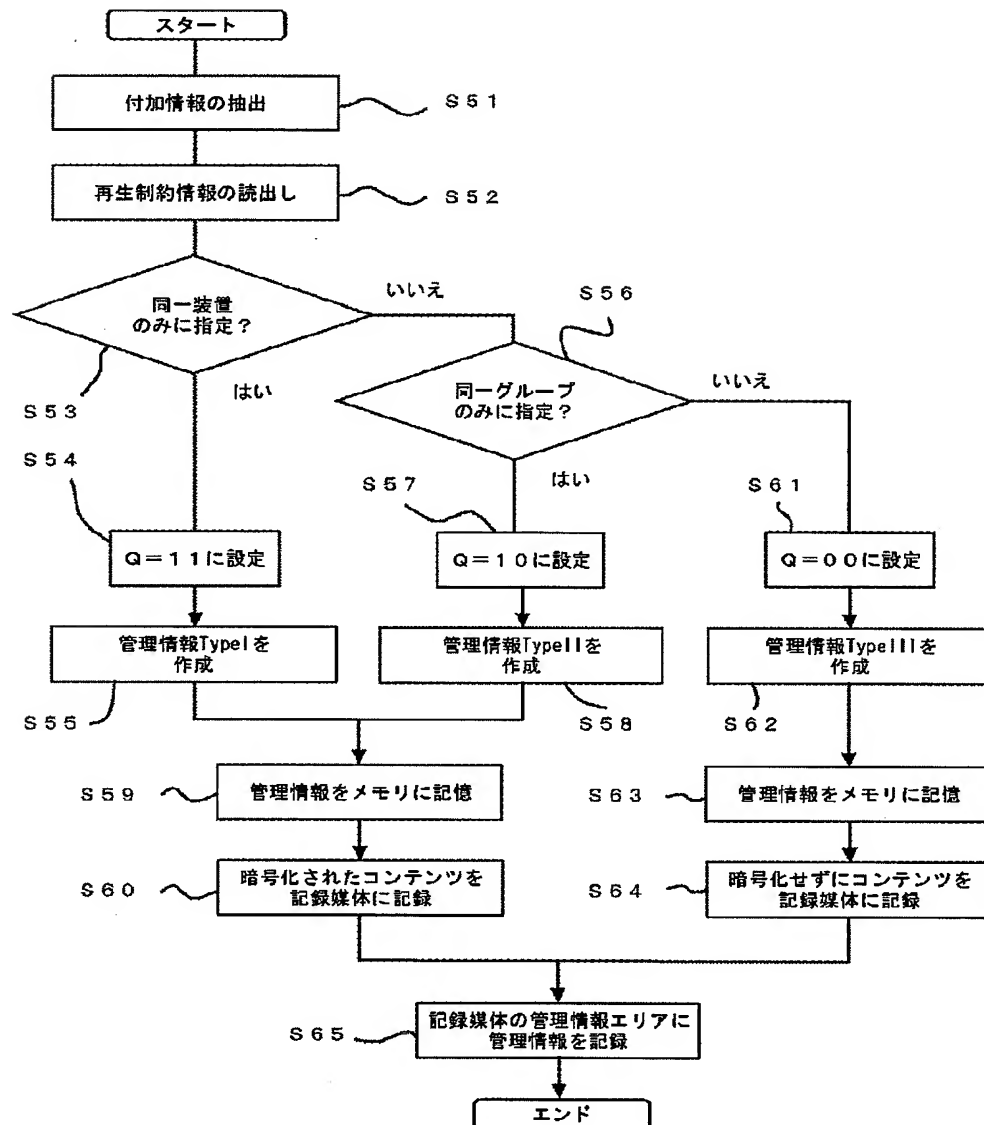
【図 7】



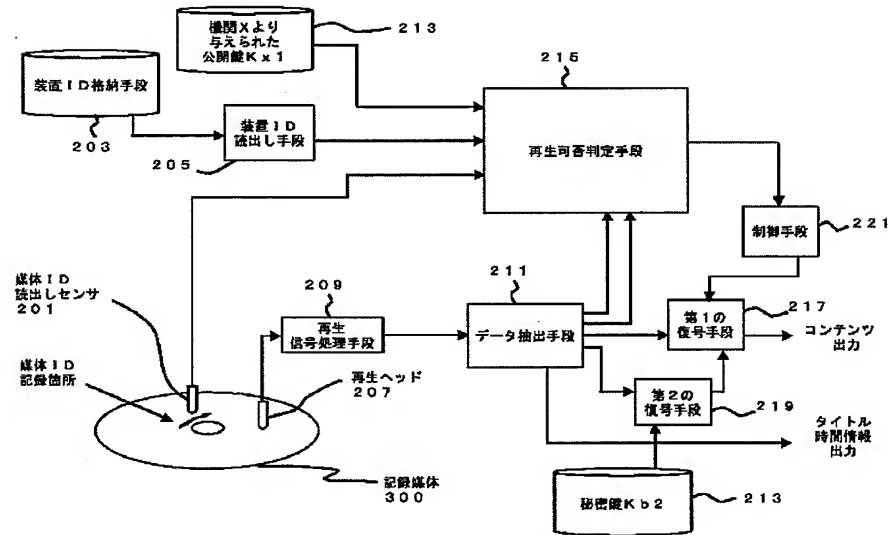
【図 8】



【図9】



【図11】



フロントページの続き

Fターム(参考) 5B017 AA06 BA09 BB00 CA00 CA06  
CA09  
5B065 BA03 BA07 CA11 PA04 PA13  
PA14  
5C053 FA13 GB06 GB11 JA01 JA21  
KA05  
5D044 AB05 AB07 BC04 CC06 DE29  
DE49 DE50 EF05 FG18 GK12  
HL02 HL08  
5J104 AA09 AA13 LA03 LA06 NA05  
PA14